Proteção Infantil Online na América Latina

Riscos, Marcos de Referência e Respostas de Política Pública

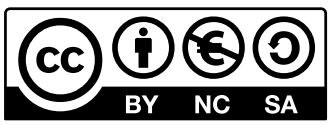
DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks Google

kriptos LUMU netskope paloalto Resecurity Schneider Electric SISAP SOPHOS

TANIUM tenable Trellix TrendAI whalemate zscaler



Resumo Executivo

A proteção infantil online (COP, na sigla em inglês) tornou-se um desafio central da governança digital na América Latina. À medida que crianças e adolescentes passam uma parte cada vez maior de suas vidas online, a região precisa ampliar a conectividade significativa e, ao mesmo tempo, garantir que os ambientes digitais sejam seguros, protegidos, respeitosos da privacidade e apropriados para a idade. Os riscos online, incluindo o aliciamento online de menores (grooming), a exploração e o abuso sexual infantil, os conteúdos nocivos, as violações de privacidade, a desinformação, o ciberbullying e os danos amplificados algoritmicamente, estão crescendo em escala e complexidade, especialmente à medida que a inteligência artificial e outras tecnologias emergentes transformam o ecossistema digital.

Os países da América Latina não partem do zero. Muitos já adotaram leis de proteção de dados, estratégias de cibersegurança, programas de alfabetização digital, mecanismos de denúncia e iniciativas de segurança infantil. Vários países já começaram a mostrar avanços importantes, com abordagens que vão desde a proteção de dados baseada em direitos e campanhas educativas até marcos mais amplos de responsabilização de plataformas e cibersegurança. No entanto, a implementação permanece desigual, e as abordagens nacionais fragmentadas limitam a capacidade da região para responder eficazmente a danos que são inerentemente transfronteiriços.

O relatório identifica várias lacunas persistentes: definições legais inconsistentes, obrigações divergentes para as plataformas, estratégias de cibersegurança com atenção limitada a riscos específicos para crianças e adolescentes, capacidades desiguais de fiscalização, cooperação transfronteiriça lenta e a dificuldade de implementar comprovação de idade e moderação de conteúdos de forma que protejam a privacidade e a liberdade de expressão. Esses desafios impõem uma carga pouco realista sobre famílias, educadores e comunidades para gerenciar riscos que exigem respostas coordenadas de caráter jurídico, técnico, institucional e do setor privado.

Os marcos internacionais do UNICEF, da UIT, do ACNUDH, da CEPAL e de outros oferecem uma base sólida para a ação regional. Esses marcos enfatizam os direitos da criança, a segurança desde a concepção e a privacidade desde a concepção, a governança multissetorial, a alfabetização digital, o apoio às vítimas e a aplicação coordenada da lei. Os exemplos de política pública da Austrália, da União Europeia, do Reino Unido e da Índia, assim como de países da América Latina, também

ilustram diferentes modelos para operacionalizar a responsabilização das plataformas, o design apropriado para a idade, a comprovação de idade e a supervisão regulatória.

A conclusão central é que a América Latina não precisa de um modelo único e uniforme para proteger crianças e adolescentes online, mas sim de maior harmonização. Os países devem preservar a flexibilidade necessária para refletir seus sistemas jurídicos e contextos culturais nacionais, ao mesmo tempo em que se alinham em torno de princípios interoperáveis, padrões técnicos compartilhados e mecanismos coordenados de fiscalização. Entre as ações prioritárias estão o desenvolvimento de um marco modelo, a harmonização de definições e salvaguardas essenciais, a criação de padrões regionais de denúncia e intercâmbio de evidências, a promoção de mecanismos de comprovação de idade que preservem a privacidade, o fortalecimento dos processos de assistência jurídica mútua, o estabelecimento de pontos focais de segurança online, o investimento em laboratórios técnicos compartilhados e capacitação, e a incorporação da governança multissetorial e das avaliações de impacto em direitos humanos na formulação de políticas. Proteger crianças e adolescentes online não é um exercício regulatório pontual. É um compromisso contínuo de governança que exige que governos, indústria, sociedade civil, educadores, famílias e instituições regionais trabalhem em conjunto. Ao combinar interoperabilidade jurídica, boas práticas de cibersegurança, salvaguardas de privacidade, participação infantil e cooperação regional, a América Latina pode construir uma abordagem mais coerente e sustentável que proteja crianças e adolescentes contra danos, ao mesmo tempo em que lhes permita se beneficiar plenamente das oportunidades da era digital.

Sumário

Introdução

O mundo está cada vez mais interconectado, e o acesso à internet sustenta hoje o desenvolvimento econômico, a educação e a participação social. Na América Latina, a rápida adoção digital entre as populações jovens ampliou as oportunidades de aprendizagem, comunicação e inclusão, ao mesmo tempo em que expôs crianças e adolescentes a uma gama crescente de riscos online, incluindo o uso nocivo de redes sociais, o uso indevido de dados e a privacidade, o aliciamento online (grooming), a exploração sexual, a exposição à desinformação e os conteúdos amplificados algoritmicamente que podem afetar negativamente a saúde mental e o desenvolvimento. Apesar da importância reconhecida da conectividade, estima-se que dois terços das crianças em idade escolar do mundo ainda não têm acesso à internet em casa, o que evidencia desigualdades persistentes que também se refletem na região.[1]

Embora a conectividade digital ofereça importantes benefícios sociais e econômicos, suas implicações para a saúde mental e física, a privacidade, a educação e o bem-estar geral de crianças e adolescentes permanecem desiguais e dependentes do contexto.[2] Ao longo da última década, o debate de política pública sobre proteção infantil online evoluiu de um enfoque estreito, centrado no acesso e na alfabetização digital, para uma ênfase mais ampla na responsabilização das plataformas, na proteção de dados, na cibersegurança e no design apropriado para a idade, impulsionado em grande medida pela crescente evidência sobre os perigos do maior uso online e seus impactos sociais adversos de longo prazo. Os governos da América Latina começaram a responder por meio de diversas abordagens, entre elas o fortalecimento de marcos de proteção de dados para menores de idade, a atualização de estratégias de cibersegurança, a introdução de obrigações para plataformas e a expansão de iniciativas de proteção infantil e alfabetização digital. No entanto, esses esforços continuam fragmentados, com variações significativas nas definições legais, na capacidade de fiscalização e na coordenação institucional.

A inteligência artificial (IA) e outras tecnologias emergentes provavelmente amplificam tanto as

[1] https://www.unicef.org/innocenti/reports/childhood-digital-world
[2] https://www.unicef.org/innocenti/reports/childhood-digital-world

oportunidades quanto os riscos, e poderiam ampliar as lacunas existentes caso não sejam abordadas de forma proativa.[3] Na América Latina, onde os marcos jurídicos, as abordagens de governança digital e os contextos culturais variam amplamente, esses desafios são particularmente complexos e cada vez mais transfronteiriços.

Este documento analisa como os países da região estão abordando a proteção infantil online na interseção entre a governança digital e a cibersegurança, destacando desafios comuns, lacunas de política pública e áreas de divergência. Também analisa o papel dos marcos internacionais e da cooperação regional, e propõe caminhos práticos para uma maior harmonização, incluindo padrões interoperáveis, mecanismos de aplicação transfronteiriça e iniciativas de fortalecimento de capacidades. Enfrentar esses desafios exigirá uma ação coordenada entre governos, indústria e sociedade civil para garantir que crianças e adolescentes possam participar do ambiente digital de forma segura, protegida e equitativa.

[3] https://www.cgdev.org/blog/three-reasons-why-ai-may-widen-global-inequality

Principais lacunas e tensões que impedem uma COP eficaz na América Latina

O ambiente digital está se tornando cada vez mais central para praticamente todos os aspectos da vida de crianças e adolescentes, incluindo educação, interação social, acesso a serviços governamentais e participação na vida cívica.[4] Em toda a América Latina, os esforços para expandir a conectividade têm sido uma prioridade central de política pública, refletindo a relação amplamente reconhecida entre o acesso à internet e o crescimento econômico, a inovação e a inclusão social.[5] As operadoras de telecomunicações e os provedores de serviços de internet (ISPs) desempenharam papel fundamental na ampliação dessa conectividade, investindo em infraestrutura e possibilitando maior participação na economia digital.[6], [7] De fato, uma conectividade confiável à internet é cada vez mais entendida como um indicador-chave de desenvolvimento, pois permite o acesso a informações, mercados e serviços públicos.[8], [9]

No entanto, essa rápida expansão do acesso digital nem sempre é acompanhada por sistemas igualmente robustos para proteger crianças e adolescentes online. Embora a conectividade gere benefícios econômicos e sociais significativos, ela também introduz um conjunto paralelo de riscos que afetam de forma desproporcional os usuários mais jovens.[10] A maior exposição às redes sociais tem sido associada a resultados negativos para a saúde mental, enquanto os ambientes online têm facilitado novas formas de dano, incluindo a exploração sexual e o aliciamento online (grooming), a propagação de desinformação e informações falsas, o uso indevido de dados e privacidade, e os conteúdos amplificados algoritmicamente que

---

[4] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[5] https://openknowledge.worldbank.org/entities/publication/483cab21-85be-544f-93c6-302e094b2dfe

[6] https://publications.iadb.org/en/strategies-and-business-models-improving-broadband-connectivity-latin-america-and-caribbean

[7] https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/

[8] https://www.cepal.org/en/publications/45835-childhood-and-adolescence-digital-age-comparative-report-kids-online-surveys

[9] https://blogs.worldbank.org/en/digital-development/can-internet-access-lead-improved-economic-outcomes

[10] https://www.unicef.org/documents/keeping-children-safe-online

podem influenciar o comportamento e o desenvolvimento.[11], [12] Esses riscos são agravados pela escala, pela velocidade e pela natureza transfronteiriça das plataformas digitais.

Em muitos casos, os marcos de política pública e regulação da região têm tido dificuldade em acompanhar esses desafios em constante evolução. As abordagens fragmentadas e pouco desenvolvidas de proteção infantil online frequentemente deixam famílias, educadores e comunidades gerenciando riscos complexos com apoio limitado. A expectativa de que lidem com essa situação por conta própria não é realista, dada a sofisticação técnica e institucional necessária para abordá-la de forma eficaz. Como resultado, lacunas e tensões significativas continuam a impedir uma resposta regional coerente.

Um dos desafios mais persistentes é a fragmentação das definições legais e das obrigações regulatórias entre os países, particularmente em relação às restrições etárias, ao que constitui conteúdo nocivo e às responsabilidades atribuídas às plataformas e aos fabricantes de dispositivos. Essa falta de alinhamento gera incerteza tanto para reguladores quanto para atores da indústria, complica a aplicação das normas e enfraquece a responsabilização. Da mesma forma, regimes divergentes de proteção de dados e privacidade, somados a capacidades limitadas de fiscalização, reduzem, em alguns casos, a capacidade das autoridades de proteger as informações pessoais de crianças e adolescentes e responder eficazmente a violações.

A cooperação transfronteiriça continua sendo outra fragilidade crítica. A atividade nociva online frequentemente ultrapassa fronteiras nacionais, mas os mecanismos de assistência jurídica mútua, compartilhamento de evidências e esforços coordenados de remoção ou rastreamento técnico costumam ser lentos, inconsistentes ou subutilizados. Para operadores de rede e provedores de serviços, essa fragmentação gera desafios operacionais ao responder a solicitações legais e implementar medidas de segurança em múltiplas jurisdições. Isso é agravado ainda mais por desafios técnicos, incluindo a necessidade de implementar sistemas de verificação ou comprovação de idade que não dependam da coleta intrusiva de dados, bem como a dificuldade de moderar conteúdos em escala em múltiplos idiomas, dialetos e contextos culturais presentes na região.

[11] https://law.stanford.edu/2024/05/20/social-media-addiction-and-mental-health-the-growing-concern-for-youth-well-being/

[12] https://www.hopkinsmedicine.org/health/wellness-and-prevention/social-media-and-mental-health-in-children-and-teens

Ao mesmo tempo, os esforços para fortalecer a proteção infantil online devem equilibrar cuidadosamente direitos e objetivos de política pública concorrentes. Regulamentações excessivamente amplas ou mal concebidas correm o risco de comprometer a liberdade de expressão, restringir o acesso à informação ou incentivar as plataformas a adotar medidas drásticas, como remoção excessiva de conteúdo ou bloqueios generalizados. Essas tensões evidenciam a necessidade de abordagens mais equilibradas e respeitadoras dos direitos, capazes de mitigar danos de forma eficaz sem gerar consequências indesejadas.

Em conjunto, esses desafios apontam para a necessidade de maior coordenação regional e interoperabilidade de políticas. Marcos jurídicos mais harmonizados, padrões técnicos alinhados e mecanismos estruturados de colaboração público-privada podem ajudar a reduzir a fragmentação, melhorar os resultados de aplicação das normas e oferecer expectativas mais claras para os atores da indústria que operam em múltiplas jurisdições.

Desafios de cibersegurança e operacionais na COP

À medida que a conectividade digital se torna uma característica definidora da vida moderna, a proteção de crianças e adolescentes online é cada vez mais determinada não apenas por considerações sociais e regulatórias, mas também pela segurança subjacente dos sistemas e infraestruturas digitais. A cibersegurança e a proteção infantil online estão profundamente interligadas. Vulnerabilidades em plataformas, dispositivos e redes podem ser exploradas para facilitar danos como o aliciamento online (grooming), a exploração sexual, violações de dados envolvendo menores de idade e a manipulação de crianças e adolescentes por meio de conteúdo malicioso ou amplificado algoritmicamente. A proliferação de dispositivos conectados, como smartphones, plataformas de videogames e brinquedos habilitados para internet, ampliou ainda mais a superfície potencial de ataque, introduzindo novos riscos quando padrões de segurança frágeis podem expor crianças e adolescentes à

vigilância, exploração ou coleta não autorizada de dados. Nesse contexto, proteger crianças e adolescentes online exige não apenas moderação de conteúdo e supervisão regulatória, mas também práticas robustas de cibersegurança incorporadas em todo o ecossistema digital.

Apesar dessa interseção evidente, as abordagens nacionais na América Latina variam significativamente quanto à medida em que as estratégias de cibersegurança abordam explicitamente riscos específicos para crianças e adolescentes. Embora alguns países tenham começado a incorporar elementos de proteção infantil em marcos mais amplos de cibersegurança, muitas estratégias continuam focadas em infraestrutura crítica, segurança econômica e crimes cibernéticos em geral, com atenção limitada às vulnerabilidades específicas da infância. No plano operacional, persistem lacunas em áreas-chave como mecanismos de denúncia seguros e acessíveis, preservação eficaz de evidências e sistemas coordenados de resposta a incidentes que integrem forças de segurança, agências de cibersegurança e serviços de proteção infantil. Fortalecer a proteção nesse âmbito exigirá uma colaboração mais estreita entre governos e setor privado, além de melhor compartilhamento de informações e protocolos mais claros de resposta intersetorial. Desenvolver essas capacidades é essencial para garantir que os esforços de cibersegurança contribuam de forma significativa para ambientes digitais mais seguros para crianças e adolescentes em toda a região.

Marcos globais e normas internacionais

Os esforços para promover a segurança infantil online são cada vez mais moldados por uma combinação de marcos internacionais e respostas nacionais de política pública. Os marcos globais, incluindo aqueles desenvolvidos por organizações como o Fundo das Nações Unidas para a Infância (UNICEF) e a União Internacional de Telecomunicações (UIT), estabeleceram princípios orientadores para a proteção de crianças e adolescentes em ambientes digitais, enfatizando abordagens baseadas em direitos, governança multissetorial e participação infantil.[13] Esses marcos fornecem uma base importante para países que buscam equilibrar os benefícios da conectividade com a necessidade de mitigar danos.

[13] https://www.unicef.org/documents/guidelines-industry-child-online-protection

Ao mesmo tempo, governos em todo o mundo e na América Latina vêm traduzindo esses princípios em políticas nacionais por meio de uma série de medidas legais e regulatórias, incluindo disposições específicas de proteção de dados para crianças e adolescentes, obrigações para plataformas, restrições etárias e iniciativas de alfabetização digital. No entanto, a interpretação e a implementação dessas normas variam consideravelmente entre jurisdições, refletindo diferenças nos sistemas jurídicos, capacidades institucionais e prioridades sociais.

Esse cenário em evolução evidencia tanto oportunidades quanto tensões. Embora os marcos internacionais promovam maior alinhamento e padrões compartilhados, as abordagens nacionais frequentemente divergem na forma como equilibram objetivos concorrentes, como privacidade versus comprovação eficaz de idade, ou liberdade de expressão versus moderação de conteúdo e segurança infantil. Compreender como essas normas globais influenciam e são adaptadas aos contextos nacionais é fundamental para identificar caminhos rumo a uma proteção infantil online mais coerente e eficaz na região.

Marcos internacionais

Diretrizes da UNICEF e da UIT para a indústria sobre proteção infantil online[14]

As Diretrizes da UNICEF e da UIT para a indústria sobre proteção infantil online oferecem um marco global reconhecido e não vinculante sobre como os atores do setor privado — incluindo operadoras de telecomunicações, provedores de serviços de internet e plataformas digitais — devem respeitar e apoiar os direitos de crianças e adolescentes no ambiente digital. Desenvolvidas por meio de um processo multissetorial, as diretrizes enfatizam uma abordagem baseada em direitos, alinhada à Convenção sobre os Direitos da Criança das Nações Unidas e aos Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos.

O marco estabelece cinco áreas centrais de atuação para a indústria: integrar os direitos da criança às políticas e à governança corporativa; implementar processos para detectar e combater material de abuso sexual infantil; projetar ambientes digitais mais seguros e apropriados para a idade; promover a alfabetização digital e o uso responsável entre crianças, adolescentes e seus responsáveis;

[14] https://www.unicef.org/media/66616/file/industry-guidelines-for-online-childprotection.pdf

e utilizar a tecnologia para apoiar a participação infantil e o engajamento cívico.[15]

De forma importante, as diretrizes reconhecem a responsabilidade compartilhada dos atores da indústria tanto na mitigação de danos quanto na promoção de experiências positivas online, incentivando as empresas a incorporar a proteção infantil ao desenvolvimento de produtos, às práticas operacionais e à colaboração intersetorial. Também oferecem recomendações específicas por setor para diferentes partes do ecossistema de TIC, incluindo ISPs, operadoras móveis, provedores de conteúdo e plataformas, refletindo os diversos papéis que esses atores desempenham na cadeia de valor digital. Em conjunto, as diretrizes funcionam como uma referência global flexível, que ajuda a alinhar as práticas empresariais aos padrões internacionais de direitos da criança, ao mesmo tempo em que permite a adaptação a diferentes contextos regulatórios e regionais.

Comentário Geral nº 25 (2021) do ACNUDH sobre os direitos da criança em relação ao ambiente digital[16]

O Comentário Geral nº 25 (2021) do Alto Comissariado das Nações Unidas para os Direitos Humanos (ACNUDH) sobre os direitos da criança em relação ao ambiente digital fornece orientação autorizada sobre como a Convenção sobre os Direitos da Criança (CDC) se aplica em contextos digitais. Afirma que os direitos de crianças e adolescentes se aplicam integralmente online, incluindo os direitos à privacidade, à proteção contra danos, ao acesso à informação, à educação e à participação. O marco enfatiza que os Estados têm a obrigação de proteger crianças e adolescentes contra riscos online, como exploração, abuso e conteúdos nocivos, ao mesmo tempo em que devem garantir que as medidas adotadas não restrinjam indevidamente o acesso à informação ou a liberdade de expressão.

O Comentário Geral defende uma abordagem holística e baseada em direitos para a governança digital, que inclua regimes de proteção de dados centrados na criança, padrões de design apropriado para a idade e mecanismos de responsabilização para provedores de serviços digitais. Também ressalta a importância da

[15] https://merlin.obs.coe.int/download/7025/pdf
[16] https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

responsabilidade empresarial, exigindo que as empresas realizem processos de devida diligência para identificar, prevenir e mitigar riscos para crianças e adolescentes. De forma importante, destaca a necessidade de acesso inclusivo, alfabetização digital e participação significativa de crianças e adolescentes nos processos de formulação de políticas que os afetam. Em síntese, o documento constitui uma referência global fundamental para orientar governos no equilíbrio entre proteção, empoderamento e direitos no ambiente digital.

CEPAL: Infância e adolescência na era digital[17]

A Comissão Econômica para a América Latina e o Caribe (CEPAL) destaca que a transformação digital da região apresenta tanto oportunidades significativas para a inclusão quanto desafios estruturais persistentes, especialmente para crianças, adolescentes e populações vulneráveis. Embora o acesso à internet tenha se expandido consideravelmente, permanecem profundas desigualdades em conectividade, qualidade de acesso e habilidades digitais, o que limita a capacidade de muitas crianças e adolescentes de se beneficiarem plenamente do ambiente digital. O relatório ressalta que a inclusão digital deve ir além do acesso para abranger acessibilidade, uso significativo e desenvolvimento de competências digitais, especialmente na educação. Ao mesmo tempo, a CEPAL enfatiza a necessidade de marcos mais sólidos de governança digital para abordar riscos emergentes, incluindo proteção de dados, cibersegurança e uso seguro de plataformas digitais. Defende abordagens coordenadas de política pública, investimento em infraestrutura e cooperação regional para reduzir lacunas e garantir que a transformação digital apoie o desenvolvimento sustentável e inclusivo. A análise também ressalta a importância de alinhar as estratégias nacionais com marcos regionais e internacionais mais amplos, adaptando ao mesmo tempo as políticas aos contextos locais.

Em geral, o relatório reforça que alcançar uma inclusão digital equitativa e segura na América Latina requer políticas integradas que equilibrem acesso, proteção e fortalecimento de capacidades, com especial atenção a crianças, adolescentes e outros grupos em situação de risco.

[17] https://repositorio.cepal.org/server/api/core/bitstreams/51f4dc9b-9bde-4358-bd68-98275f64583d/content

Modelo Nacional de Resposta da WeProtect para pôr fim à exploração e ao abuso sexual infantil online[18]

O Modelo Nacional de Resposta da Aliança Global WeProtect oferece uma abordagem estruturada para que os governos previnam e respondam à exploração e ao abuso sexual infantil online (CSEA, na sigla em inglês). Apresenta um modelo abrangente e sistêmico baseado em seis domínios fundamentais: política e governança, justiça criminal, apoio às vítimas, engajamento da indústria, sociedade e prevenção, e coordenação e cooperação. O marco enfatiza que uma proteção infantil online eficaz exige ação integrada entre instituições, incluindo forças de segurança, serviços de proteção infantil, reguladores e atores do setor privado.

Uma característica central do modelo é seu foco na colaboração multissetorial e em papéis e responsabilidades claramente definidos, garantindo que governos, indústria e sociedade civil trabalhem de forma coordenada. Também destaca a importância do fortalecimento de capacidades, do compartilhamento de dados e da prontidão operacional, incluindo mecanismos de denúncia, investigação e apoio às vítimas.
O marco inclui um modelo de maturidade que permite aos países avaliar suas capacidades atuais e identificar lacunas, apoiando uma abordagem gradual para fortalecer as respostas nacionais. Em geral, serve como uma ferramenta prática de implementação que ajuda os países a traduzir princípios internacionais em sistemas coordenados e acionáveis para enfrentar a exploração e o abuso infantil online.

Exemplos de políticas nacionais

Embora os marcos internacionais estabeleçam um conjunto compartilhado de princípios e expectativas para a proteção infantil online, sua eficácia depende, em última instância, de como são traduzidos em leis, regulamentos e práticas operacionais nacionais. Em todo o mundo, os governos vêm adaptando essas normas internacionais a respostas de política doméstica que refletem seus sistemas jurídicos, capacidades institucionais e prioridades sociais. Esse processo resultou em um panorama diverso de abordagens para proteger crianças e adolescentes online, oferecendo lições valiosas sobre boas práticas emergentes e lacunas persistentes na implementação.

[18] https://www.weprotect.org/resources/frameworks/model-national-response/

Austrália: Online Safety Act 2021[19]

A Online Safety Act 2021 da Austrália estabelece um marco regulatório abrangente para enfrentar uma ampla gama de danos online, com forte foco na proteção de crianças, adolescentes e usuários vulneráveis. A legislação concede poderes ampliados à eSafety Commissioner para exigir a remoção rápida de conteúdos nocivos, incluindo material de ciberbullying dirigido a crianças e adolescentes, abuso baseado em imagens e conteúdo ilegal ou seriamente nocivo.[20] Introduz padrões exigíveis de segurança online para plataformas e provedores de serviços, exigindo que adotem medidas proativas para reduzir a exposição a material nocivo e melhorar os mecanismos de denúncia e resposta.

A lei também inclui o marco Basic Online Safety Expectations, que estabelece requisitos mínimos para provedores de serviços digitais em matéria de segurança dos usuários, transparência e responsabilização. De forma importante, cria caminhos para enfrentar danos emergentes como o aliciamento online (grooming), a exploração sexual e a difusão não consentida de imagens íntimas, ao mesmo tempo em que apoia as vítimas por meio de mecanismos de denúncia e reparação. A legislação reflete uma abordagem sistêmica e baseada em riscos, que combina supervisão regulatória, obrigações da indústria e proteções para usuários a fim de mitigar danos e manter o acesso aos serviços digitais.

Em geral, a lei é amplamente considerada um modelo prático e exigível para operacionalizar a proteção infantil online, demonstrando como os governos podem traduzir princípios de alto nível em ferramentas regulatórias concretas e autoridade institucional.

União Europeia: Resolução do Parlamento Europeu 2693/2026[21]

O Parlamento Europeu solicitou uma ação mais forte em nível da União Europeia para combater o ciberbullying, em particular para proteger melhor crianças e jovens online. A iniciativa enfatiza a necessidade de marcos jurídicos mais claros, maior responsabilização das plataformas e melhores mecanismos de denúncia e apoio às vítimas. Aborda danos como o assédio online, o abuso psicológico e a disseminação de conteúdos nocivos, ao mesmo tempo

[19] https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation
[20] https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/esafety-commissioner
[21] https://www.europarl.europa.eu/news/en/press-room/20260423IPR41845/parliament-wants-stronger-action-against-cyberbullying-in-the-eu

em que promove ações coordenadas entre os Estados-membros. A proposta também destaca a importância de medidas de prevenção, alfabetização digital e cooperação transfronteiriça, refletindo uma abordagem mais proativa e harmonizada para enfrentar o ciberbullying na UE.

União Europeia: tecnologias de comprovação de idade em escala da UE[22]

A abordagem comum da Comissão Europeia sobre tecnologias de comprovação de idade em escala da UE propõe um marco coordenado para proteger menores de idade do acesso a conteúdos inadequados para a sua idade online, particularmente no âmbito da Lei de Serviços Digitais (DSA). A iniciativa promove o desenvolvimento e a implantação de soluções de comprovação de idade que preservem a privacidade, com o objetivo de verificar se um usuário está acima ou abaixo de determinada idade sem exigir a coleta excessiva de dados pessoais. Essa abordagem busca mitigar danos como a exposição a conteúdo nocivo ou inadequado, o aliciamento online (grooming) e a exploração, ao mesmo tempo em que aborda preocupações sobre proteção de dados e privacidade do usuário.
O marco enfatiza a interoperabilidade e a padronização em toda a UE, incentivando o uso de sistemas de identidade digital confiáveis e credenciais reutilizáveis para garantir consistência entre plataformas e serviços. Também reflete uma abordagem baseada em riscos e proporcional, que exige que as plataformas implementem salvaguardas apropriadas de acordo com a natureza de seus serviços e os riscos que representam para menores de idade. De forma importante, a iniciativa equilibra os objetivos de proteção infantil com os direitos fundamentais, particularmente a privacidade e a minimização de dados, promovendo tecnologias que reduzam o rastreamento e a elaboração de perfis.

A abordagem da UE demonstra como os governos podem avançar soluções escaláveis e tecnicamente viáveis para a comprovação de idade que se alinhem a marcos regulatórios mais amplos, oferecendo um modelo para integrar a proteção infantil em sistemas de identidade digital e governança de plataformas.

[22] https://digital-strategy.ec.europa.eu/en/library/commission-sets-out-common-approach-eu-wide-age-verification-technologies

Reino Unido: Online Safety Act 2023[23]

A Online Safety Act 2023 do Reino Unido estabelece um regime regulatório abrangente voltado a reduzir os danos online, com forte ênfase na proteção de crianças e adolescentes. A legislação impõe deveres de cuidado estatutários às plataformas online, exigindo que avaliem e mitiguem proativamente os riscos associados a conteúdos nocivos, particularmente para menores de idade. As plataformas devem implementar medidas de segurança apropriadas para a idade, incluindo moderação de conteúdo mais robusta, configurações de segurança padrão para crianças e adolescentes, e mecanismos para evitar a exposição a materiais nocivos, como pornografia, conteúdo de autolesão e abuso online.

A lei concede ao regulador de comunicações, a Ofcom, autoridade significativa de supervisão e fiscalização, incluindo a capacidade de estabelecer padrões de segurança, exigir relatórios de transparência e impor multas substanciais por descumprimento. Também introduz exigências para que as plataformas enfrentem conteúdo ilegal e danos

[23] https://www.legislation.gov.uk/ukpga/2023/50

prioritários, incluindo a exploração e o abuso sexual infantil, o aliciamento online (grooming) e o ciberbullying, ao mesmo tempo em que melhora os mecanismos de denúncia e reparação para os usuários.

De forma importante, a legislação adota uma abordagem baseada em riscos e proporcional, exigindo que as empresas adaptem as proteções de acordo com a escala e a natureza de seus serviços. Ao mesmo tempo, busca equilibrar a proteção infantil com considerações de liberdade de expressão e privacidade, incorporando salvaguardas para evitar excessos. Em geral, a lei representa um modelo operacional robusto para traduzir princípios de proteção infantil online em obrigações exigíveis para plataformas e supervisão regulatória.

Índia: Information Technology Rules (Intermediary Guidelines and Digital Media Ethics Code), 2021 (atualizadas em 2023)[24]

As Information Technology Rules da Índia (Intermediary Guidelines and Digital Media Ethics Code), 2021 (modificadas em 2023), estabelecem um marco regulatório para intermediários online, com disposições que enfrentam danos que afetam crianças, adolescentes e usuários vulneráveis. As regras impõem obrigações de devida diligência às plataformas, exigindo que removam conteúdo ilícito dentro de prazos específicos, incluindo material relacionado ao abuso sexual infantil, exploração e outros conteúdos nocivos. Os intermediários também devem implementar mecanismos de reparação de queixas, designar responsáveis pela conformidade e permitir que os usuários denunciem conteúdo nocivo de forma eficiente.

O marco introduz obrigações adicionais para plataformas de maior porte, incluindo medidas de monitoramento proativo e exigências de rastreabilidade para certos tipos de conteúdo, voltadas a enfrentar questões como abuso online, desinformação e exploração. Também inclui disposições para restringir o acesso a conteúdo inadequado para a idade e fortalecer a responsabilização dos editores de mídia digital por meio de um código de ética e uma estrutura de supervisão.

Embora as regras busquem mitigar danos como a exploração online, a disseminação de conteúdo nocivo e o abuso, também suscitaram debates importantes sobre privacidade, criptografia e liberdade de expressão, particularmente em relação às exigências de rastreabilidade. Em geral, o marco representa um modelo

[24] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

orientado pela conformidade que enfatiza a responsabilização das plataformas, a remoção rápida de conteúdos e a supervisão governamental como ferramentas-chave para enfrentar danos online.

Panorama regional: como os países da América Latina abordam a COP

Os marcos internacionais e exemplos nacionais mencionados demonstram uma crescente convergência em torno de princípios centrais, como a governança baseada em direitos, a coordenação multissetorial, a segurança desde a concepção e a responsabilização das plataformas. No entanto, sua implementação varia significativamente entre regiões. Na América Latina, os países se encontram em diferentes estágios de maturidade política e institucional, refletindo disparidades em marcos jurídicos, capacidade regulatória, infraestrutura digital e disponibilidade de recursos. Como resultado, as abordagens de proteção infantil online na região continuam desiguais, com alguns países avançando em estratégias abrangentes enquanto outros ainda desenvolvem políticas fundamentais. Apesar dessas diferenças, existe uma clara oportunidade — e necessidade — de que todos os países se alinhem a esses princípios globais compartilhados, adaptando-os a contextos locais enquanto avançam para abordagens mais consistentes, eficazes e interoperáveis para proteger crianças e adolescentes online. Os países a seguir estão entre aqueles que começaram a abordar esses temas.

Argentina

A abordagem da Argentina para a proteção infantil online se apoia em seu marco consolidado de proteção de dados e se complementa com legislação penal específica, iniciativas de conscientização pública e uma estratégia emergente de cibersegurança. A Lei nº 25.326 de Proteção de Dados Pessoais fornece a base jurídica central, estabelecendo princípios como consentimento, limitação de finalidade e segurança de dados, que se aplicam aos dados de menores de idade, mas sem criar um regime plenamente diferenciado e específico para a infância.[25], [26] A autoridade nacional de proteção de dados (AAIP) buscou preencher essa lacuna por meio de orientações não vinculantes e iniciativas públicas, em particular seu programa “Nuestro

[25] https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790
[26] https://termly.io/resources/articles/argentinas-personal-data-protection-act/

Mundo Digital", que promove alfabetização digital, conscientização sobre privacidade e salvaguardas práticas para crianças, adolescentes, famílias e educadores.[27] A AAIP também emitiu posicionamentos sobre comprovação de idade e privacidade infantil que enfatizam proporcionalidade, minimização de dados e alinhamento com padrões regionais e internacionais, refletindo uma abordagem cautelosa e baseada em direitos para implementar salvaguardas técnicas.[28]

No âmbito penal e preventivo, a Lei nº 27.590 (a "Lei Mica Ortega") desempenha papel central ao exigir programas de educação e conscientização sobre o aliciamento online (grooming), evidenciando uma ênfase de política pública na prevenção por meio de escolas e campanhas públicas, em vez de uma regulação centrada nas plataformas.[29] Do ponto de vista da cibersegurança, as capacidades da Argentina se estruturam em torno do CERT.ar, que fornece resposta nacional a incidentes, monitoramento de ameaças e coordenação entre setores, formando a base operacional para enfrentar riscos digitais, inclusive aqueles que afetam menores de idade.[30] Esses esforços são ainda contextualizados pelo plano federal de prevenção a crimes cibernéticos e gestão estratégica da cibersegurança para 2025–2027, que integra gestão de riscos cibernéticos, coordenação institucional e fortalecimento de capacidades, embora sem um enfoque específico robusto na infância.[31]

Em geral, a postura da Argentina é caracterizada por uma base de proteção de dados orientada por direitos, complementada por medidas de segurança infantil impulsionadas por educação e conscientização, além de infraestrutura geral de cibersegurança. Em comparação com modelos mais prescritivos, depende em maior medida de orientações, iniciativas de política pública e ferramentas de direito penal, com menor ênfase em obrigações vinculantes para plataformas ou marcos regulatórios abrangentes específicos para a infância.

---

[27] https://www.argentina.gob.ar/aaip/nuestro-mundo-digital-guia-pedagogica-y-guia-para-adolescentes

[28] https://iapp.org/news/a/argentinas-appi-creates-ai-transparency-and-protection-of-personal-data-program

[29] https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto

[30] https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar

[31] https://www.boletinoficial.gob.ar/detalleAviso/primera/319722/20250116

Brasil

O Brasil adotou uma abordagem cada vez mais abrangente e integrada de proteção infantil online, que combina obrigações legais, orientação regulatória e estratégia nacional de cibersegurança. No centro está a Lei nº 15.211/2025 ("ECA Digital"), que estabelece um marco baseado em direitos e fundamentado no melhor interesse de crianças e adolescentes, impondo obrigações afirmativas aos provedores de serviços digitais para garantir segurança desde a concepção e privacidade desde a concepção.[32] A lei exige que as plataformas implementem medidas como design apropriado para a idade, configurações padrão de alta privacidade, controles parentais e avaliação contínua de riscos de funcionalidades que possam expor menores de idade a danos, incluindo sistemas algorítmicos.[33] Essas obrigações são operacionalizadas por meio do Decreto nº 12.880/2026, que cria uma arquitetura federal coordenada de fiscalização e denúncia, esclarece responsabilidades institucionais e incorpora a proteção infantil online em uma estrutura de política nacional mais amplia liderada pelo Ministério da Justiça.[34] [35] Os materiais governamentais, incluindo a iniciativa "ECA Digital" do Ministério, enfatizam um modelo preventivo e sistêmico que combina regulação, conscientização pública e cooperação intersetorial.[36]

No campo da governança de dados, o Brasil aproveita seu regime existente de proteção de dados sob a Lei Geral de Proteção de Dados Pessoais (LGPD)[37], com a Autoridade Nacional de Proteção de Dados (ANPD)[38], recentemente elevada de autoridade a agência federal, emitindo orientações detalhadas sobre o tratamento de dados pessoais de crianças e adolescentes.[39] Isso inclui exigências de base legal, limitação de finalidade e salvaguardas reforçadas, junto com uma expectativa clara de privacidade por padrão e restrições à elaboração de perfis e à publicidade comportamental.[40] Como complemento, a orientação preliminar de 2026 da ANPD sobre comprovação de idade confiável destaca uma abordagem técnica que equilibra eficácia com

---

[32] https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm
[33] https://www.hrw.org/news/2025/09/17/brazil-passes-landmark-law-to-protect-children-online
[34] https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12880.htm
[35] https://www.dataguidance.com/news/brazil-president-signs-two-decrees-regulating-digital
[36] https://www.dataguidance.com/news/brazil-president-signs-two-decrees-regulating-digital
[37] https://lgpd-brazil.info/
[38] https://www.gov.br/anpd/pt-br
[39] https://iapp.org/news/a/anpd-becomes-regulatory-agency-a-turning-point-for-brazilian-data-protection-compliance
[40] https://www.gov.br/planalto/pt-br/acompanhe-o-planalto/noticias/2025/09/lula-sanciona-lei-que-protege-criancas-na-internet-e-anuncia-medidas-para-ampliar-concorrencia-e-infraestrutura-digital

proporcionalidade e preservação da privacidade, incentivando métodos baseados em riscos e desincentivando a coleta excessiva de dados. No plano da cibersegurança, a Estratégia Nacional de Cibersegurança do Brasil (E-Ciber 2025) reforça a proteção de populações vulneráveis, incluindo crianças e adolescentes, por meio da promoção de infraestrutura digital segura, capacidade de resposta a incidentes e coordenação entre atores públicos e privados.[41] [42] Por fim, a implementação conta na prática com o apoio de parcerias da sociedade civil, como a SaferNet Brasil, que oferece canais amplamente utilizados de denúncia, linhas de apoio e recursos educativos, ilustrando como o Brasil combina mandatos legais com mecanismos operacionais de denúncia, apoio às vítimas e alfabetização digital.[43] Em conjunto, esses elementos refletem uma postura em camadas que integra política pública, salvaguardas técnicas e coordenação institucional para enfrentar riscos a crianças e adolescentes em ambientes digitais.

Chile

A abordagem do Chile em relação à proteção infantil online é determinada por um marco maduro de cibersegurança, juntamente com uma transição significativa em seu regime de proteção de dados. A Política Nacional de Cibersegurança 2023–2028, liderada pela Agência Nacional de Cibersegurança (ANCI), estabelece uma estratégia coordenada e baseada em riscos centrada na proteção de infraestrutura crítica, resposta a incidentes e colaboração intersetorial.[44] Operacionalmente, o CSIRT nacional fornece resposta a incidentes em nível nacional, monitoramento de ameaças e orientação pública, formando a base técnica para gerenciar riscos digitais, inclusive aqueles que afetam menores de idade. Embora esses instrumentos não sejam específicos para a infância, contribuem para um ambiente digital seguro que sustenta uma segurança online mais ampla.[45]

O marco de proteção de dados do Chile é atualmente regido pela Lei nº 19.628, que fornece uma base geral para o tratamento de dados pessoais, mas oferece disposições limitadas

[41] https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber
[42] https://depp.oecd.org/policies/BRA2214
[43] https://new.safernet.org.br/denuncie
[44] https://anci.gob.cl/pncs-2023-2028/
[45] https://csirt.gob.cl/

específicas para a infância.[46] Isso mudará com a Lei nº 21.719, que entrará em vigor em dezembro de 2026 e estabelece um regime modernizado de proteção de dados, além de criar uma autoridade supervisora dedicada.[47] Espera-se que a nova lei fortaleça salvaguardas, responsabilização e supervisão, com implicações mais claras para os dados de crianças e adolescentes e os serviços digitais.[48] No âmbito social e de política pública, iniciativas como Kids Online Chile 2022 e o programa de Cidadania Digital do Ministério da Educação dão visibilidade aos riscos enfrentados por crianças e adolescentes online e promovem alfabetização digital, uso responsável e conscientização entre estudantes, educadores e famílias.[49] [50]

Em geral, a postura do Chile combina instituições sólidas de cibersegurança com um marco de proteção de dados em evolução e iniciativas de segurança infantil centradas na educação. Seu modelo enfatiza a capacidade institucional e o desenvolvimento de políticas públicas, e é provável que a próxima reforma de proteção de dados desempenhe papel fundamental no avanço de uma governança digital mais robusta e sensível à infância.

México

A abordagem do México em relação à proteção infantil online reflete uma convergência crescente entre o planejamento de cibersegurança, a governança das telecomunicações e a política de direitos da criança. No plano estratégico, o Plano Nacional de Cibersegurança 2025–2030[51], apoiado pela Agência de Transformação Digital e Telecomunicações (ATDT)[52], enquadra a cibersegurança como uma questão de resiliência nacional e segurança pública, com relevância implícita para a proteção de populações vulneráveis, incluindo menores de idade.[53] Operacionalmente, o CERT-MX fornece capacidades de resposta a incidentes, monitoramento de ameaças e coordenação entre os setores público e privado, formando a base da infraestrutura técnica de cibersegurança do México. Embora esses instrumentos não sejam específicos para a infância, contribuem para um ambiente mais amplo de mitigação de riscos digitais que sustenta a segurança online.[54]

---

[46] https://www.bcn.cl/leychile/navegar?idNorma=141599
[47] https://www.bcn.cl/leychile/navegar?i=1209272
[48] https://resguard-solutions.com/blog/es/chile-data-protection-law-21719-guide/
[49] https://www.unicef.org/chile/informes/kids-online-chile-2022
[50] https://ciudadaniadigital.mineduc.cl/
[51] https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030
[52] https://www.gob.mx/atdt/
[53] https://www.gob.mx/atdt/comunicacion/liderara-mexico-ciberresiliencia-en-la-region-con-plan-nacional-de-ciberseguridad
[54] https://www.gob.mx/gncertmx

As proteções voltadas a crianças e adolescentes se desenvolvem de forma mais explícita por meio de canais institucionais e de política pública. O SIPINNA (Sistema Nacional de Proteção Integral de Crianças e Adolescentes) lidera os esforços federais em segurança infantil online, emitindo orientações sobre uso seguro da internet, alfabetização digital e prevenção de riscos, frequentemente em colaboração com parceiros internacionais como o UNICEF México, que enfatiza uma abordagem educativa e baseada em direitos.[55] Em paralelo, o marco de telecomunicações do México desempenha um papel na configuração de responsabilidades em nível de plataforma e rede, particularmente em torno do acesso, do conteúdo e das proteções para os usuários.[56] A proteção de dados é regida por leis federais aplicáveis tanto ao setor público quanto ao privado, que estabelecem princípios como consentimento, limitação de finalidade e salvaguardas de segurança, incluindo considerações reforçadas para os dados de menores de idade.

Em geral, a postura do México combina infraestrutura de cibersegurança, regulação de telecomunicações e política de direitos da criança, mas permanece menos centralizada e prescritiva do que a de outros países. Sua força reside na coordenação institucional e nos esforços de educação pública, enquanto sua estrutura de governança de dados em evolução e sua dependência de ferramentas gerais de cibersegurança evidenciam desafios persistentes para desenvolver um regime coeso de segurança digital específico para a infância.

Peru

A abordagem do Peru em relação à proteção infantil online se apoia em um marco jurídico dedicado que aborda especificamente o uso seguro e responsável das TIC por crianças e adolescentes, complementado pela legislação geral de proteção de dados e por estruturas nacionais de cibersegurança. A Lei nº 30254, modificada pela Lei nº 31664 e implementada por meio do Decreto Supremo nº 093–2019–PCM, estabelece obrigações para promover ambientes digitais seguros, prevenir riscos online como o aliciamento online (grooming) e a exploração, e fomentar a coordenação entre governo, setor privado e sociedade civil.[57] O marco dá especial ênfase à conscientização, à educação e à responsabilidade compartilhada, em vez de impor obrigações diretas

[55] https://www.gob.mx/sipinna/articulos/ciberseguridad-para-ninas-ninos-y-adolescentes-en-el-ecosistema-digital
[56] https://www.gob.mx/crt/es/que-hacemos
[57] https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292146–30254

extensas às plataformas digitais, sendo operacionalizado por meio de políticas nacionais e iniciativas interinstitucionais.

O regime de proteção de dados do Peru, sob a Lei nº 29733, fornece a base para a privacidade e a governança de dados pessoais, incluindo princípios como consentimento, limitação de finalidade e salvaguardas de segurança aplicáveis aos dados de menores de idade.[58] Embora não seja específico para a infância, apoia os esforços mais amplos de segurança online ao regular como os dados pessoais são coletados e processados. Em matéria de cibersegurança, o Centro Nacional de Segurança Digital e funções relacionadas de CSIRT fornecem coordenação nacional para resposta a incidentes, monitoramento de riscos e política de segurança digital, contribuindo para um ecossistema digital mais seguro em geral.
A proteção voltada a crianças e adolescentes é reforçada por esforços governamentais de educação pública e coordenação, incluindo orientações oficiais para famílias sobre uso seguro da internet e iniciativas como a Alianza Nacional por una Internet Segura, que reúne instituições públicas e atores privados para promover conscientização e práticas preventivas.[59] Em geral, a postura do Peru enfatiza educação, coordenação interinstitucional e proteções jurídicas específicas para menores de idade, respaldadas por marcos gerais de privacidade e cibersegurança, mas com uma ênfase comparativamente menor em obrigações vinculantes em nível de plataformas.

Uruguai

A abordagem do Uruguai em relação à proteção infantil online se baseia em um marco sólido de proteção de dados, apoiado por uma governança coordenada de cibersegurança e uma ênfase notável em alfabetização digital e prevenção. A Lei nº 18.331 de Proteção de Dados Pessoais estabelece o regime jurídico central, incorporando princípios como consentimento, limitação de finalidade e segurança de dados, e é supervisionada pela autoridade de proteção de dados (URCDP), que fornece supervisão institucional e orientação.[60] [61] Embora a lei não seja exclusivamente específica para a infância, aplica-se aos dados de menores de idade e se complementa com interação regulatória e orientação pública que reforçam as proteções de privacidade em ambientes digitais.
No plano da cibersegurança, o Uruguai

[58] https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733
[59] https://www.gob.pe/20720-seguridad-digital-para-ninos-ninas-y-adolescentes
[60] https://www.impo.com.uy/bases/leyes/18331-2008
[61] https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/uruguayan-law-protection-personal-data-and-habeas-data-action-ldpd-2024-09-25_en

desenvolveu uma estrutura coerente de governança liderada pela Agesic, que coordena a estratégia nacional de cibersegurança, a gestão de riscos e a colaboração interinstitucional.[62] Operacionalmente, o CERTuy atua como a equipe nacional de resposta a incidentes, oferecendo monitoramento de ameaças, canais de denúncia e procedimentos de resposta acessíveis tanto para instituições quanto para o público.[63] Suas regras e processos definidos de relato de incidentes contribuem para uma abordagem estruturada e transparente no tratamento de ameaças digitais, incluindo aquelas que podem afetar crianças e adolescentes.

A proteção voltada a crianças e adolescentes é particularmente visível nas políticas de prevenção do Uruguai. A estratégia de cidadania digital do Ceibal integra segurança online, uso responsável da tecnologia e habilidades digitais ao sistema educacional, dirigida a estudantes, professores e famílias.[64] Isso é reforçado por evidências empíricas do estudo Kids Online Uruguay 2022, que documenta comportamentos, riscos e estratégias de enfrentamento de crianças e adolescentes online, fundamentando políticas e intervenções educacionais baseadas em evidências.[65] Em geral, a postura do Uruguai reflete um modelo equilibrado que combina proteção de dados, capacidade institucional de cibersegurança e fortes esforços preventivos impulsionados pela educação, com uma força particular em integrar a segurança infantil online à sua agenda nacional de inclusão digital e educação.

Considerações regionais

Em conjunto, esses exemplos nacionais mostram tanto avanços significativos quanto oportunidades de melhoria em toda a região. Embora exista um claro alinhamento com princípios globais, particularmente em torno da governança baseada em direitos, da prevenção e da coordenação institucional, os caminhos de implementação diferem de acordo com tradições jurídicas, capacidade institucional e prioridades de política pública. Essa diversidade não é exclusiva da América Latina; países de outras regiões também estão experimentando diferentes combinações regulatórias, arranjos institucionais e abordagens técnicas para a proteção infantil online. Não surgiu um único modelo definitivamente

[62] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/
[63] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/certuy
[64] https://ceibal.edu.uy/institucional/articulos/lanzamiento-nueva-estrategia-nacional-de-ciudadania-digital-2024–2028/
[65] https://www.unicef.org/uruguay/informes/informe-kids-online-uruguay-2022

"correto", e as tentativas de impor uma solução uniforme correm o risco de ignorar os fatores contextuais que determinam tanto os riscos quanto as intervenções viáveis.

Consequentemente, o caminho mais eficaz não está em convergir para um único modelo, mas sim em uma harmonização cuidadosa. As abordagens nacionais devem continuar tomando como referência marcos internacionais e padrões compartilhados, garantindo interoperabilidade, cooperação transfronteiriça e proteções básicas para crianças e adolescentes em um ambiente digital inerentemente global. Ao mesmo tempo, essas abordagens devem permanecer adaptáveis aos contextos locais, refletindo sistemas jurídicos nacionais, considerações culturais e realidades de recursos. Equilibrar o alinhamento global com a relevância contextual será fundamental para construir regimes de proteção infantil online resilientes, coerentes e eficazes, tanto dentro da América Latina quanto no âmbito de um panorama internacional mais amplo e em evolução.

Soluções práticas de política pública, técnicas e de governança para a harmonização regional

Avançar a proteção infantil online na América Latina exige passar do alinhamento de alto nível em torno de princípios para mecanismos práticos que permitam coordenação, interoperabilidade e responsabilização compartilhada. Com base nos marcos internacionais existentes e nas diversas abordagens nacionais descritas anteriormente, esta seção propõe soluções acionáveis e adaptáveis em nível regional. Essas recomendações são concebidas de forma modular, permitindo que os países adotem elementos comuns enquanto os adaptam a seus sistemas jurídicos, capacidades institucionais e ambientes de risco nacionais.

Harmonização jurídica e regulatória

Um passo fundamental para a coerência regional é o desenvolvimento de um marco modelo de COP ou lei de referência que estabeleça padrões mínimos centrais. Em vez de prescrever legislação idêntica,

esse modelo deveria definir elementos básicos fundamentais: definições harmonizadas (incluindo "criança", "adolescente" e idade de consentimento digital), salvaguardas mínimas de proteção de dados para menores de idade, obrigações de denúncia obrigatória para danos graves online (como exploração sexual infantil e aliciamento online), e disposições de porto seguro para plataformas condicionadas ao cumprimento de exigências de devido processo e transparência. Sua elaboração deve estar alinhada com orientações internacionais estabelecidas, incluindo os marcos da UIT e do UNICEF, bem como com princípios amplamente aceitos de privacidade e direitos humanos.

É fundamental incentivar os países a adotar princípios interoperáveis em vez de linguagem estatutária idêntica. Essa abordagem permite a compatibilidade jurídica entre fronteiras, facilitando a cooperação e a aplicação, ao mesmo tempo em que preserva a flexibilidade para a adaptação nacional. Organismos ou fóruns regionais podem apoiar esse processo por meio da emissão de orientações interpretativas, cláusulas modelo e atualizações periódicas que reflitam riscos e tecnologias em evolução.

Interoperabilidade técnica e padrões

O alinhamento jurídico deve ser complementado pela interoperabilidade técnica para garantir que os sistemas projetados para detectar, denunciar e responder a danos possam funcionar sem fricções entre jurisdições. Uma área prioritária é o desenvolvimento de um padrão regional de denúncia: um esquema de dados compartilhado para documentar incidentes como exploração sexual infantil, aliciamento online e outros danos de alto risco. Isso permitiria relatórios consistentes por parte das plataformas, recepção mais fluida pelas autoridades e um tratamento mais eficiente de casos transfronteiriços. Junto a isso, protocolos seguros para o intercâmbio de evidências (que incorporem criptografia, salvaguardas de cadeia de custódia e proteções de privacidade) são essenciais para investigações transfronteiriças oportunas e legais.
Paralelamente, a América Latina se beneficiaria de padrões técnicos comuns para design apropriado para a idade e comprovação de idade que preserve a privacidade. Em vez de depender de métodos de verificação intrusivos ou inconsistentes, os países podem promover abordagens baseadas em minimização de dados, como provas criptográficas ou atestações de atributos mínimos que confirmem faixas etárias sem expor a identidade completa. Expectativas

padronizadas de transparência das plataformas, apoiadas por APIs compartilhadas ou ferramentas de relatório, podem fortalecer ainda mais a responsabilização, permitindo que reguladores e pesquisadores acessem dados comparáveis sobre moderação de conteúdo, relatórios de abuso e resultados de mitigação de riscos.

Aplicação e cooperação transfronteiriça

Dada a natureza inerentemente transnacional dos danos online, fortalecer os mecanismos de aplicação transfronteiriça é fundamental. O desenvolvimento de modelos padronizados de Assistência Jurídica Mútua (MLA, na sigla em inglês) adaptados a casos de COP pode reduzir significativamente atrasos e fricções processuais. Esses modelos deveriam incluir canais expeditos para questões urgentes de segurança infantil, com prazos claros e vias de escalonamento. O estabelecimento de pontos focais designados de COP dentro de agências de aplicação da lei, autoridades de proteção de dados e redes judiciais pode agilizar ainda mais a comunicação e a coordenação.

Capacitação e serviços compartilhados

As disparidades em capacidade institucional continuam sendo uma barreira significativa para uma implementação eficaz. Enfrentá-las exige investimento sustentado em iniciativas regionais de fortalecimento de capacidades. Poderia ser desenvolvido um currículo de capacitação padronizado que cobrisse aspectos jurídicos, técnicos e operacionais da COP para promotores, juízes, forças de segurança, equipes CERT e organizações de proteção infantil. Sua oferta por meio de centros regionais de capacitação ou plataformas online garantiria escalabilidade e acessibilidade.

Os serviços compartilhados oferecem uma forma eficiente de ampliar capacidades em países com menos recursos. Laboratórios técnicos regionais poderiam fornecer análise forense avançada, processamento de evidências digitais e serviços de apoio às vítimas.

Governança multissetorial e prestação de contas

Marcos eficazes de COP dependem de estruturas de governança inclusivas que reúnam reguladores, indústria, sociedade civil e defensores dos direitos da criança. Os países deveriam considerar a criação de órgãos de supervisão multissetoriais tanto em nível nacional quanto regional, encarregados de monitorar a conformidade das plataformas, avaliar a eficácia das políticas e assessorar sobre riscos emergentes. Esses órgãos podem melhorar a transparência,

construir confiança pública e garantir que diversas perspectivas se reflitam na tomada de decisões.

Em nível regional, esses mecanismos podem facilitar o aprendizado entre pares e a comparação de avanços, permitindo que os países comparem progresso, identifiquem lacunas e coordenem respostas. Os processos de relato periódico e prestação pública de contas devem ser integrados a essas estruturas para manter o impulso e a credibilidade.

Salvaguardas de privacidade e considerações de direitos humanos

Por fim, todos os esforços de harmonização devem se basear em salvaguardas sólidas para proteger os direitos fundamentais. Devem ser exigidas avaliações de impacto em direitos humanos (AIDH) obrigatórias para intervenções relacionadas à COP, particularmente aquelas que envolvam tecnologias sensíveis como comprovação de idade, filtragem de conteúdo ou ferramentas de vigilância. Essas avaliações devem analisar proporcionalidade, necessidade e possíveis consequências não desejadas, garantindo que as medidas concebidas para proteger crianças e adolescentes não comprometam direitos mais amplos à privacidade, à expressão e ao acesso à informação.

Igualmente importante é incluir as vozes de crianças e adolescentes na concepção e na avaliação de políticas. Mecanismos de participação significativa, como painéis consultivos juvenis, consultas e pesquisas participativas, podem fornecer informações valiosas sobre experiências vividas e riscos emergentes. Incorporar essas perspectivas não apenas fortalece a relevância das políticas, mas também reforça a base de direitos dos esforços de COP.

Conclusão

A proteção infantil online já não é um tema periférico de política digital; é um componente central da governança digital, da cibersegurança, dos direitos da criança e do desenvolvimento inclusivo. À medida que crianças e adolescentes na América Latina passam uma parte cada vez maior de suas vidas online, a região enfrenta uma dupla responsabilidade: expandir a conectividade significativa e, ao mesmo tempo, garantir que os ambientes digitais sejam seguros, protegidos, respeitosos dos direitos e apropriados para a idade. O desafio não consiste simplesmente em reduzir o dano depois que ele ocorre, mas em construir sistemas que previnam o abuso, protejam a privacidade, fortaleçam a resiliência e permitam que crianças e adolescentes participem plenamente do mundo digital.

Este documento mostra que os países da América Latina não partem do zero. Em toda a região, os governos desenvolveram leis de proteção de dados, estratégias de cibersegurança, iniciativas de educação pública, mecanismos de denúncia e marcos emergentes de responsabilização de plataformas. Os modelos internacionais e marcos globais também oferecem uma base sólida. No entanto, o progresso permanece desigual, e as abordagens fragmentadas limitam a eficácia dos esforços nacionais frente a riscos inerentemente transfronteiriços. A região precisa agora avançar de iniciativas isoladas para uma harmonização prática, princípios compartilhados, padrões interoperáveis, aplicação coordenada, instituições mais sólidas e fortalecimento sustentado de capacidades. Isso inclui avançar marcos jurídicos interoperáveis baseados em princípios comuns, desenvolver padrões técnicos regionais para denúncia e intercâmbio de evidências, promover abordagens de comprovação de idade que preservem a privacidade, fortalecer mecanismos de cooperação transfronteiriça, investir em serviços regionais compartilhados e capacitação, e estabelecer estruturas de governança multissetorial que apoiem a transparência e a responsabilização.

Não existe um único modelo “correto” de proteção infantil online. Cada país deve adaptar soluções ao seu sistema jurídico, capacidade institucional, cultura e ecossistema digital. Mas a flexibilidade nacional não deve se traduzir em fragmentação regional. Uma abordagem mais coerente, baseada em padrões internacionais de direitos humanos, salvaguardas de privacidade, boas práticas de cibersegurança e participação significativa de crianças e adolescentes, pode ajudar os países a protegê-los e, ao mesmo tempo, preservar a abertura, a inovação e o acesso à informação. Portanto,

os esforços de harmonização regional deveriam priorizar princípios interoperáveis em vez de leis idênticas, permitindo que os países se alinhem em torno de objetivos compartilhados mantendo flexibilidade nacional. Ao mesmo tempo, salvaguardas como as avaliações de impacto em direitos humanos e os mecanismos participativos que incorporem as vozes de crianças e adolescentes devem continuar sendo centrais no desenvolvimento e na implementação de políticas.

Os governos devem modernizar os marcos jurídicos e fortalecer a capacidade de fiscalização. A indústria deve incorporar segurança desde a concepção e privacidade desde a concepção em produtos e serviços utilizados por crianças e adolescentes. As plataformas também devem apoiar relatórios de transparência padronizados e implementar medidas de design apropriado para a idade que minimizem a coleta desnecessária de dados e protejam a privacidade infantil. A sociedade civil, os educadores, as famílias e as organizações de proteção infantil devem receber recursos como parceiros essenciais, em vez de serem deixados sozinhos diante da gestão de riscos. As instituições e parceiros regionais devem apoiar ferramentas compartilhadas, capacitação, intercâmbio de evidências e padrões técnicos que tornem a cooperação mais rápida e eficaz.

Proteger crianças e adolescentes online não é um projeto regulatório pontual; é um compromisso contínuo de governança. O ambiente digital continuará evoluindo, e os riscos também. A América Latina tem a oportunidade de construir uma abordagem regional prática, interoperável e respeitosa dos direitos: uma que proteja crianças e adolescentes contra danos enquanto os capacita a se beneficiar das oportunidades da era digital. Ao combinar interoperabilidade jurídica, coordenação técnica, cooperação transfronteiriça, governança inclusiva e sólidas salvaguardas de privacidade e direitos humanos, a região pode avançar rumo a um modelo mais eficaz e sustentável de proteção infantil online que reflita tanto as realidades regionais quanto as boas práticas globais.


DIGI
AMERICAS